PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-026935
(43)Date of publication of application : 25.01.2002

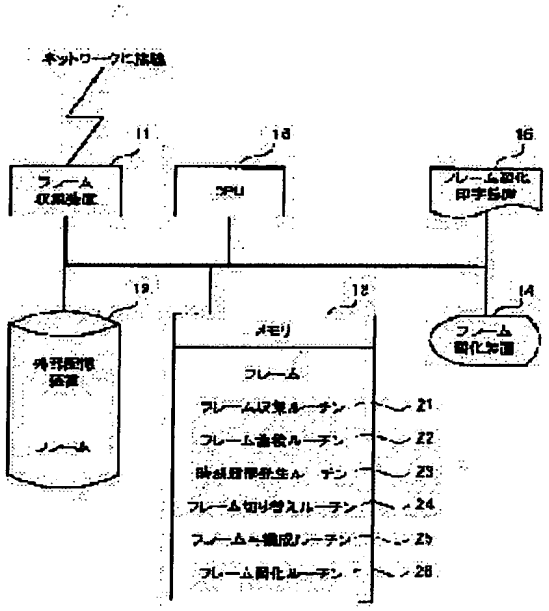
(51)Int.Cl. H04L 12/28
H04L 12/24
H04L 12/26
H04L 29/14
H04N 7/18

(21)Application number : 2000-210536
(22)Date of filing : 11.07.2000

(71)Applicant : LAC CO LTD
(72)Inventor : SAKAI YORIYUKI

(54) FRAME MONITORING DEVICE AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a frame monitoring device that visually grasps frames at an optional time distributed through a network and stored or frames distributed at present in real time so as to analyze a network fault or an illegal access.
SOLUTION: The frame monitoring device is connected to a network in which plural communication units (computers or the like) are connected mutually and monitors frames distributed through the network. The device is provided with a frame collection device 11 that collects frames distributed through the network in real time, an external storage device 12 that gives a time calendar to the frames and sequentially stores them, a frame illustration device 14 or a frame illustration printer 15 that reads the stored frames, reconfigures the frames in a frame reconfiguration routine 25 to reconfigure the frames on the basis of prescribed attribute and visually displays a state of the reconfigured frames.



LEGAL STATUS

[Date of request for examination] 26.06.2007

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－26935
（P2002－26935A）
(43)公開日　平成14年１月25日(2002.1.25)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード*(参考)
Ｈ０４Ｌ　12/28		Ｈ０４Ｎ　7/18	Ｚ	５Ｃ０５４
12/24		Ｈ０４Ｌ　11/00	３１０Ｄ	５Ｋ０３０
12/26		11/08		５Ｋ０３３
29/14		13/00	３１３	５Ｋ０３５
Ｈ０４Ｎ　7/18				

審査請求　未請求　請求項の数４　ＯＬ　（全 10 頁）

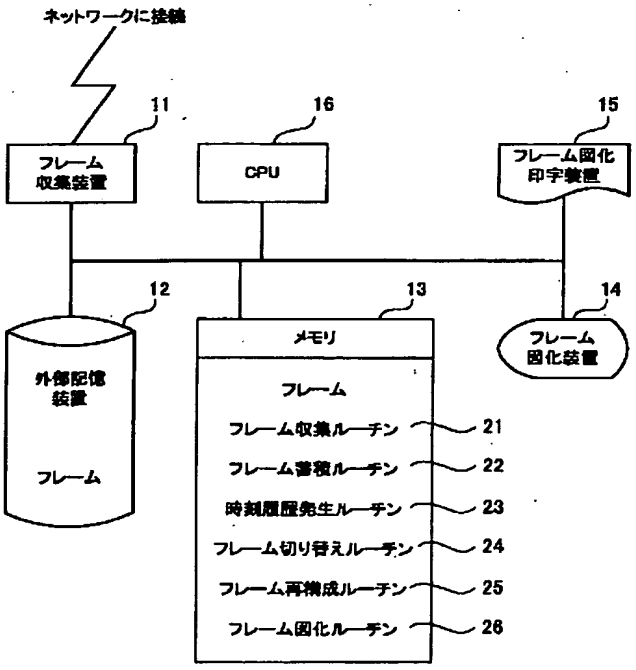
(21)出願番号　特願2000－210536(P2000－210536)
(22)出願日　平成12年７月11日(2000.7.11)

(71)出願人　500072884
株式会社ラック
東京都港区新橋３丁目26番４号　新橋相互ビル304号
(72)発明者　坂井　順行
東京都江東区青海２－45タイム24ビル３Ｆ　株式会社ラック内
(74)代理人　100104880
弁理士　古部　次郎　（外１名）

最終頁に続く

(54)【発明の名称】　フレーム監視装置および記憶媒体

(57)【要約】
【課題】　ネットワーク内を流れる蓄積された任意の時間のフレーム、または現在流れているフレームをリアルタイムで視覚的に把握し、ネットワーク障害や不正アクセス等に対する分析を行う。
【解決手段】　複数台の通信機器(コンピュータ等)を相互接続するネットワークに接続され、このネットワーク上を流れるフレームを監視するフレーム監視装置であって、ネットワークを流れるフレームをリアルタイムで収集するフレーム収集装置１１と、フレームに時刻暦を付与して順次、蓄積する外部記憶装置１２と、蓄積されたフレームを読み出し、所定の属性に基づいて再構成するためのフレーム再構成ルーチン２５にてフレームを再構成し、再構成されたフレームの状況を視覚的に表示するフレーム図化装置１４またはフレーム図化印字装置１５を備えた。



1

【特許請求の範囲】

【請求項１】　複数台の通信機器を相互接続するネットワークに接続され、当該ネットワーク上を流れるフレームを監視するフレーム監視装置であって、
前記フレームに時刻暦を付与して順次、蓄積する蓄積手段と、
前記蓄積手段により蓄積されたフレームを所定の属性に基づいて再構成するフレーム再構成手段と、
前記フレーム再構成手段により再構成された前記フレームの状況を視覚的に表示する表示手段と、を備えたことを特徴とするフレーム監視装置。

【請求項２】　前記フレーム再構成手段は、前記蓄積手段に蓄積されたフレームを時系列順でリストアップし、
前記表示手段は、前記フレーム再構成手段によってリストアップされたフレームに対し、前記通信機器の論理的位置、フレームの通過時刻、および複数のフレームにおける相互の関連性に関わる情報を視覚的要素にて表示することを特徴とする請求項１記載のフレーム監視装置。

【請求項３】　複数台の通信機器を相互接続するネットワークに接続され、当該ネットワーク上を流れるフレームを監視するフレーム監視装置であって、
前記ネットワークを流れるフレームをリアルタイムで収集するフレーム収集手段と、
前記フレーム収集手段により収集されたフレームに対し、前記通信機器の論理的位置、および複数のフレームにおける相互の関連性を視覚的に表示する表示手段と、を備えたことを特徴とするフレーム監視装置。

【請求項４】　コンピュータに実行させるプログラムを当該コンピュータの入力手段が読取可能に記憶した記憶媒体であって、
前記プログラムは、ネットワーク上を流れるフレームに対して時刻暦を付与して順次、収集する処理と、
収集された前記フレームをメモリに蓄積する処理と、
収集された前記フレームまたは蓄積された前記フレームを取得し、表示部に対して所定の通信機器間におけるフレームの通過時刻およびフレームの属性を視覚的に表示させる処理と、を前記コンピュータに実行させることを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数台の通信機器によって構築されたネットワーク内を流れるフレーム状態を把握する装置等に係り、特に、相互接続されたコンピュータ等の論理的位置、フレームの通過時刻、複数のフレームの相互関連性等を視覚的に分析、把握する装置等に関する。

【０００２】

【従来の技術】従来より、相互接続された複数台のコンピュータ間において、通信ネットワークを利用してフレームを伝送することによりデータのやり取りを行う方式

2

が一般的に採用されている。

【０００３】インターネットあるいはＬＡＮ(Local Area Network)におけるイーサネット（登録商標）を用いたコンピュータを相互接続する場合においては、ＩＰ(Internet Protocol)、ＩＰＸ/ＳＰＸ(Internetwork Packet Exchange/Sequenced)、ＮｅｔＢＥＵＩ(Netbios Extended User Interface)、ＴＣＰ(Transmission Control Protocol)、ＵＤＰ(User Datagram Protocol)等のプロトコルが知られている。これらプロトコルでは、フレームによりデータの転送を行っている。フレームは、プロトコル内容や送信元アドレス、宛先アドレス、エラーチェックを行うヘッダ部分、およびデータが格納されるボディ部分から構成されている。

【０００４】また、インターネットを含めて標準的なネットワークで用いられるプロトコルを体系的に理解するために、ＯＳＩ(Open Systems Interconnection：開放型システム間相互接続)参照モデルと対比することが一般に行われている。このＯＳＩ参照モデルでは、ビット列の伝送を行う物理層である第１層、隣接ノード間の誤りのないデータ転送を行うデータリンク層である第２層、両システム間の接続とデータ転送を行うネットワーク層である第３層、両端プロセス間のデータ転送品質保証を行うトランスポート層である第４層、対話モードの管理を行うセッション層である第５層、転送のための表現を行うプレゼンテーション層である第６層、業務に応じた情報のやり取りを行うアプリケーション層である第７層からなる７階層を定義している。上述したＴＣＰ/ＩＰは、ＯＳＩ参照モデルにおけるネットワーク層とトランスポート層に相当している。

【０００５】ここで、近年、複数台のコンピュータがＴＣＰ/ＩＰネットワーク等を用いて相互接続される場合に、例えば不正アクセスの発見等を目的としてネットワーク上でどのようなデータが流れているのかを把握することが要求されている。例えば文献１（ファイヤウォール構築「インターネットセキュリティ」D. BrentChapman著、(株)オライリージャパン）には、複数台のコンピュータがＴＣＰ/ＩＰネットワークを用いて相互接続され、相互間にフレームの伝播が見られる場合、問題発生時の証拠保全を目的として稼動中のコンピュータシステム内の状態を定期的に保存する技術について示されている。より具体的には、ハードディスク等の磁気記録媒体における内容の複製を他の磁気記録媒体に実行させ、この他の磁気記録媒体に記録された複製内容を読み出し、再生することによって問題点を調査するものである。この技術によれば、コンピュータシステム内において問題発生直前の状態への復旧を容易にし、証拠の保存、および原因と結果の因果関係を突き止めることが可能である。

【０００６】また、文献２（日経コミュニケーション１９９８年２月、３月号「トラフィックを監視せよ」）に

は、ＴＣＰ/ＩＰネットワークで構築されたネットワーク層以上のフレームを収集し、フレーム伝送の傾向を取り出す手段として、ネットワークモニタツールが紹介されている。ここでは、「ネットワークで発生するトラブルの原因を特定したり、将来のネットワークを設計する上で重要なのは、ネットワーク上でどのようなデータが流れているのかを把握することである。」と指摘されている。そして、コンピュータネットワーク上を流れるフレームの複製を定期的に他の磁気記録媒体へ行い、フレームの把握の判断材料として、全データ量(トラフィック)、全フレーム数、正常または異常なフレームの数、プロトコル別、アプリケーション別のトラフィックを元にフレームの内容分析を行うことのできるフレームのモニタリングソフトウェアが考案され、一般に利用されている。

【０００７】更に、文献３(月刊インタロップマガジン１９９９年１２月号「侵入検知システムを用いたセキュリティの監視」)には、ネットワーク型ＩＤＳ(Intrusion Detection System)として、ネットワークトラフィックやアクセス状況などをリアルタイムに解析し、不審な行為、即ち不正アクセスが行われていないかどうかを監視するシステムが紹介されている。この技術では、フレームを収集し、予め用意された不正アクセスを目的とするフレームの例である「ひな形」との比較により、不正アクセス現象が生じているかどうかをフレームの通過と同時に判断することが可能である。

【０００８】また更に、文献４(「Network Intrusion Detection Systems」 Robert Graham)では、ネットワーク型ＩＤＳが不正アクセスを目的とするフレームであると判断する際の欠点として、いくつかの問題点が指摘されている。例えば、ここでの指摘事項として、❶フレームの大きさをネットワーク型ＩＤＳが期待する大きさよりも小さくすることによる「センサへのめくらまし行為(Blind the sensor)」、❷フレームの送り出し元情報を改ざんしてフレームを送り出し、ネットワーク型ＩＤＳのフレーム伝送状況記録を無価値にしてしまう「状況記録へのめくらまし行為(Blind the event storage)」、❸フレームの数をネットワーク型ＩＤＳが処理できる以上に送り出し、フレーム収集に引き続くフレーム内容の分析機能を動作不能状態に陥らせる「サービス不能状態(Denial of Service)」、が示されている。

【０００９】

【発明が解決しようとする課題】しかしながら、前述の文献１で示された技術では、コンピュータ自身としての問題点、即ち、コンピュータ自身に記録されたエラーの中身を保全し、起こった事象を証拠として保存することはできても、ネットワークに対して、どのような異常が起こり、どのような壊れ方をしたのかを把握することは困難である。

【００１０】また、上述の文献２で示された技術では、採取されたフレームの解析方法について、単位時間あたりのフレーム数によるトラフィック量の増加程度、採取した全フレームの種類別統計に主眼を置いており、フレーム内容やフレーム内容の複製そのもの、フレームの送信順序については保全することができず、問題発生時の証拠としてのフレームの価値は十分とは言えなかった。また、フレームの傾向分析に主眼を置いているため、フレームのヘッダに規格外の実装がなされている場合や、フレームのデータ部分に誤りがある場合は、それらは全て無条件に「異常フレーム」として計数されていた。このため、どのような異常があって規格外の実装とされているのか、また、どのようなデータの誤りがあったのかを後から取り出して実際に見ることは困難であった。

【００１１】更に、上述の文献３で示された技術では、フレームを収集することによって不正アクセス現象を予め作成してある「ひな形」と比較して、フレームの通過と同時に判断することはできるが、既に通過した過去の任意のフレーム通過状態をシステム内に再現し、エラー状況を分析、判断するような機能は実装されていない。また、「ひな形」とずれがあった場合には不正アクセスを検出しにくくなるという問題がある。

【００１２】また更に、前述の文献４では、いくつかの不正アクセスに関する問題点の指摘はあるものの、これらの解決手段については何ら言及されていない。これらの問題が発生した場合、ネットワーク型ＩＤＳではリアルタイムに不正アクセス現象が生じているか否かを判定することができず、不正アクセスを放置することとなってしまう。

【００１３】本発明は、以上のような技術的課題を解決するためになされたものであって、その目的とするところは、ネットワークを利用するユーザに対して、フレームの送信元、送信先の論理的な位置関係、複数のフレームにおける時間的間隔、相互の関連性等を直感的に認識させることにある。また他の目的は、不正アクセスと疑わしいフレームを捕捉し、不正アクセス現象の証拠を収集することにある。

【００１４】

【課題を解決するための手段】かかる目的のもと、本発明は、複数台の通信機器(コンピュータ等)を相互接続するネットワークに接続され、このネットワーク上を流れるフレームを監視するフレーム監視装置であって、フレームに時刻暦を付与して順次、蓄積する蓄積手段と、この蓄積手段により蓄積されたフレームを所定の属性に基づいて再構成するフレーム再構成手段と、このフレーム再構成手段により再構成されたフレームの状況を視覚的に表示する表示手段とを備えたことを特徴としている。

【００１５】ここで、このフレーム再構成手段は、蓄積手段に蓄積されたフレームを時系列順でリストアップし、表示手段は、このフレーム再構成手段によってリストアップされたフレームに対し、通信機器の論理的位

置、フレームの通過時刻、および複数のフレームにおける相互の関連性に関わる情報を視覚的要素にて表示することを特徴とすれば、フレームの時間的な間隔や相互の関連性を直感的に理解することが可能となる点で好ましい。この通信機器の論理的位置とは、例えば、ネットワークに基づいて構成される送信先の論理的位置関係等が該当する。また、複数のフレームにおける相互の関連性とは、例えば、ＴＣＰが運ばれたフレームが流れたことや、ＩＰが通過した、ＵＤＰが通過した等の情報や、データ量の情報等が挙げられる。これらの情報を視覚的要素にて表示する際には、例えば、色分けや、線の種類、線の太さ等を異ならせて表現することができる。

【００１６】一方、本発明を他の観点から把えると、本発明は、複数台の通信機器を相互接続するネットワークに接続され、このネットワーク上を流れるフレームを監視するフレーム監視装置であって、ネットワークを流れるフレームをリアルタイムで収集するフレーム収集手段と、このフレーム収集手段により収集されたフレームに対し、通信機器の論理的位置、および複数のフレームにおける相互の関連性を視覚的に表示する表示手段とを備えたことを特徴としている。この発明によれば、フレームのヘッダに規格外の実装がなされていたり、フレームのデータフィールドに誤りがある場合等、これらの「異常フレーム」をリアルタイムに把握することができる点で優れている。

【００１７】また、本発明は、コンピュータに実行させるプログラムをこのコンピュータの入力手段が読取可能に記憶した記憶媒体であって、このプログラムは、ネットワーク上を流れるフレームに対して時刻暦を付与して順次、収集する処理と、収集されたフレームをメモリに蓄積する処理と、収集されたフレームまたは蓄積されたフレームを取得し、表示部に対して所定の通信機器間におけるフレームの通過時刻およびフレームの属性を視覚的に表示させる処理とをコンピュータに実行させることを特徴としている。この記憶媒体としては、例えばコンピュータ装置におけるＣＤ-ＲＯＭ装置にて読取可能なＣＤ-ＲＯＭ記憶媒体等が該当する。

【００１８】

【発明の実施の形態】以下、添付図面に示す実施の形態に基づいてこの発明を詳細に説明する。図１は、本実施の形態におけるシステムの全体構成を説明するための図である。この図１に示すシステムは、複数台からなるコンピュータを相互接続するためのＴＣＰ/ＩＰネットワーク等に接続され、ネットワーク上を流れるパケット等からなるフレームを監視するフレーム監視装置として構成することができる。

【００１９】図１において、符号１１はフレーム収集装置であり、ネットワークに接続されてネットワーク上を流れているフレームを収集する機能を備えている。１２は外部記憶装置であり、例えば大容量のハードディスクや、磁気テープ、光磁気ディスク等からなり、フレーム収集装置１１にて収集されたフレームを保存する機能を備えている。１３はメモリであり、ＲＡＭ等から構成され、本システムのメインメモリとして収集されたフレームを処理するのに必要な各種ルーチン等を格納している。１４はフレーム図化装置であり、収集されたフレーム情報を図化してディスプレイに表示している。１５はフレーム図化印字装置であり、プリンタ等を用いて図化された出力画像を印字することができる。また、１６はＣＰＵであり、メモリ１３に格納された各種ルーチンに基づいて中央演算装置として本システムを制御している。

【００２０】メモリ１３では、外部記憶装置１２から読み出されたフレームが一旦、蓄えられる。また、このメモリ１３には、ＣＰＵ１６等が実行する各種ルーチンとして、フレーム収集ルーチン２１、フレーム蓄積ルーチン２２、時刻履歴発生ルーチン２３、フレーム切り替えルーチン２４、フレーム再構成ルーチン２５、およびフレーム図化ルーチン２６が格納されている。

【００２１】フレーム収集ルーチン２１は、ネットワーク上を流れているフレームを収集するためのルーチンであり、このフレーム収集ルーチン２１に基づきフレーム収集装置１１が制御されてフレーム収集を可能としている。フレーム蓄積ルーチン２２は、フレーム収集装置１１により収集されたフレームを外部記憶装置１２に蓄積するためのルーチンである。時刻履歴発生ルーチン２３は、収集されるフレームに対して時刻暦を与えるためのルーチンであり、時刻暦であるタイムスタンプを発生させている。フレーム切り替えルーチン２４は、フレーム切り替え処理として、リアルタイムに流れているフレームを選択するか、または外部記憶装置１２に一旦、蓄積されたフレームを任意に取り出して再現するかを選択している。フレーム再構成ルーチン２５は、取り出された各々のフレームの再構成を行うルーチンである。ここで、フレームの再構成とは、時刻履歴発生ルーチン２３によってタイムスタンプが付与されて外部記憶装置１２に蓄積されたフレームに対し、時系列順に並べ替えたり、属性毎に揃えて並べ替えたり、フレームの出発点や到着点のコンピュータ毎に並べ替えたり、規格に沿わないフレームを抜き出す等の作業として定義できる。また、フレーム図化ルーチン２６は、フレーム図化装置１４およびフレーム図化印字装置１５のために、図化可能な様相に再構築されたフレームの図化処理を行うためのルーチンである。

【００２２】次に、本実施の形態における処理の流れを説明する。図２は本実施の形態における全体処理を説明するためのフローチャートである。図２に示すように、まず、ＴＣＰ/ＩＰネットワーク上を流れるフレームをフレーム収集装置１１にて採取する際に、一つ一つのフレームに対して、時刻履歴発生ルーチン２３にて時刻履

歴であるタイムスタンプを発生させ(ステップ１０１)、ここで発生させたタイムスタンプをフレームに対して付与しながら、フレーム収集ルーチン２１に基づいて動作するフレーム収集装置１１にて、フレームの収集がなされる(ステップ１０２)。ここで、ステップ１０１にてタイムスタンプが付与され、ステップ１０２にて収集されたフレームは、フレーム蓄積ルーチン２２によって全て外部記憶装置１２に対して蓄積される(ステップ１０３)。

【００２３】ここで、蓄積を行ったものを表示するか否かの図化選択が行われる(ステップ１０４)。即ち、図化選択によってリアルタイムに流れるフレームデータの表示か、蓄積された過去のフレームデータの表示かが選択される。このステップ１０４にて、蓄積を行ったものを表示しない場合には、フレーム切り替えルーチン２４によってリアルタイムに流れているフレームデータが選択される(ステップ１０５)。一方、ステップ１０４にて、蓄積を行ったものの表示が指示された場合には、フレーム切り替えルーチン２４によって外部記憶装置１２からフレームデータの取得がなされる(ステップ１０６)。

【００２４】ステップ１０５およびステップ１０６によりフレームデータが得られた後、表示方法の指示が与えらたか否かが判断される(ステップ１０７)。表示方法の指示が与えられていない場合には、例えば、フレーム図化装置１４に設けられたディスプレイ等を用いて表示方法の指示を促し(ステップ１０８)、表示方法の指示を待つ。ステップ１０７にて表示方法の指示がなされた場合には、フレーム再構成ルーチン２５によって、例えば、時系列順、属性毎、出発点毎、到着点毎等にフレームが再構成され(ステップ１０９)、フレーム図化ルーチン２６によりフレーム図化装置１４に対してフレームを図化する(ステップ１１０)。尚、表示方法の指示によっては、プリンタ等からなるフレーム図化印字装置１５に出力しても構わない。この一連の処理によって、ネットワーク上に流れているフレーム、若しくは外部記憶装置１２に蓄積されたフレームが、フレーム図化装置１４またはフレーム図化印字装置１５上に状態表示されるまでの一連のプロセスが終了する。

【００２５】図３は、フレーム図化装置１４等にて表示される表示例を示した図である。フレーム図化印字装置１５でも同様に表示することが可能である。ここで、フレーム図化装置１４のディスプレイ等に表示される画面は、大きく、ひな形画像を表示する画面３０と、接続状態と実際のフレームを図化するための画面４０とで構成されている。

【００２６】画面３０には、通信エリアが結線状態であるという意味を持つ通信線３１、フレーム収集装置１１の意味を持つアイコンであるフレーム収集装置アイコン３２、大型コンピュータを意味するアイコンである大型コンピュータアイコン３３、端末の意味を持つアイコンである端末アイコン３４、フレームの出発元もしくは到着先等のネットワーク仮想集合体という意味を持つネットワーク仮想集合体アイコン３５等が示されている。ユーザは、これらのアイコンを任意に選択することで、接続状態と実際のフレームを図化する画面４０を形成することができる。

【００２７】画面４０には、ユーザが画面３０で選択されたアイコンが表示されると共に、表示された複数のアイコンを通信線３１等で繋ぎ合わせたネットワークの論理的な位置付けが表示される。即ち、実際の画面への出力を行う前に、フレームを収集するＴＣＰ/ＩＰネットワークに接続されている通信機器、通信エリア、相互の接続状態の情報等を含んだ接続図４１が定義される。この接続図４１に接続する通信機器の情報には、使用するパケットの種類上での一意な識別子を含んでおく必要がある。定義した通信機器、通信エリアが、ＴＣＰ/ＩＰネットワークを用いて相互接続されている場合には、相互接続を示す識別子も定義される。この識別子は、システムの利用者によって定義可能であり、また、記録されたフレーム種別、リアルタイムに取得されるフレーム種別からも定義される。定義された通信機器、通信エリアについての視覚的情報は、フレーム図化装置１４、フレーム図化印字装置１５上では、それぞれ一つのアイコンとして表示されるものとしている。

【００２８】図３に示す例では、ユーザによるフレームの監視位置に、端末またはそれに準ずるコンピュータが合計４台、大型のコンピュータが１台、またフレーム収集するフレーム収集装置が１台、存在している。また、それらは、他の多くのコンピュータによって構成されるネットワーク仮想集合体に接続されているという論理的な位置付けを表している。接続図４１の中では、これらの接続状態を、フレーム収集装置アイコン３２、大型コンピュータアイコン３３、端末アイコン３４、ネットワーク仮想集合体アイコン３５、通信線３１で表現している。ここで、フレームが通過している場合の通信線３１は、フレームの種類や量によって太さや色を変えたり、点線等で表示することができる。また、フレームの流れる方向を点滅の移動等によって表現することも可能である。

【００２９】また、本実施の形態では、フレームの量を、データリンク層以上の全てのフレームについて集計するように定義している。そして、フレームの量を表すために、前述のデータリンク層以上を流れる全てのフレームを集計する。このように、流れているフレームの量に関しては、通信線３１の太さを変えて表示することによって、例えば最初の１秒目に３ミリ幅であったものが、次の１秒後には５ミリ幅に太くなったとすれば、通過する量が増えたということが容易に判断できる。

【００３０】更に、本実施の形態では、外部記憶装置１２にて蓄積されていたフレームや、リアルタイムに取得

されたフレームに対して、通信線３１の色を変え、即ち、予め定義された色(例えば、青、赤、黄、緑、白等)を用いて、識別子を表示できるように構成している。例えば、青はＴＣＰが運ばれているフレームが流れているものとし、赤はＴＣＰでもＵＤＰでもないフレームが通過したものとし、黄はＵＤＰが運ばれているフレームが流れているものとする。また、緑はＩＰ及びＩＣＭＰが通過したものとし、白はＩＰではないものが通過したと定義する。これらの色の中からどの色を表示するかということは、その時々に応じて見たいものを選択できるように構成することも可能である。例えば、ＴＣＰの通過について調べたい場合には、青、赤、黄のいずれかを選択することによって、フレームの通過状況を容易に調査することができる。また、ＩＰの通過について調べたい場合には、緑、白のいずれかを選択すれば良い。ここで、赤によって表現された場合には、ＴＣＰでもＵＤＰでもないフレームの通過であり、パケットの並びを狂わせて改ざんされたフレームである可能性が高い。この赤の表現によって、不正かどうかが疑わしいフレームが通過したことを認識することが可能である。尚、フレームがＴＣＰ/ＩＰネットワーク上を流れていない状態では、流れていない状態を示す色(例えばディスプレイのバックグラウンドと同色等)で、通信機器、通信エリア、相互接続を示す識別子を表示するように構成することができる。

【００３１】また、画面４０には、日付・時刻情報を表わす時刻カウンタ４３も表示される。この時刻カウンタ４３では、年、月、日、時(ＨＨ)、分(ＭＭ)、秒(ＳＳ)が表示される。時刻カウンタである年、月、日、時、分、秒については、現在表示しているフレームが通過した時間がリアルタイムで表示される。ここで、外部記憶装置１２に蓄積されたフレームを再生して表示している場合には、時刻履歴発生ルーチン２３によって付与されたタイムスタンプを読み込んで表示することとなる。リアルタイムで表示、または再生していく途中でネットワーク上を流れるフレームがなくなった場合でも、年、月、日、時、分、秒は動き続ける。

【００３２】図４は、フレーム図化装置１４等で表示される設定画面の例を示した図である。図４において、設定画面５０では、日付・時刻情報表示エリア５１、表示速度選択ボタン５２、および作動ボタン５３が表示される。この設定画面５０に対して、例えばマウス等のポインティングデバイスを用いて指定することが可能であり、また、この設定画面５０を例えば液晶タッチパネル等で構成して、ユーザによる簡易な操作入力を実現することもできる。日付・時刻情報表示エリア５１では、表示開始年月日、表示開始時刻、表示終了年月日、表示終了時刻が表示される。また、表示速度選択ボタン５２では、例えば１／１６倍速、１／８倍速、１／４倍速、１／２倍速、１倍速、２倍速、４倍速、８倍速というような任意の表示速度を選択することができる。また、作動ボタン５３では、再生ボタン５３ａ、一時停止ボタン５３ｂ、停止ボタン５３ｃ、逆再生ボタン５３ｄによって、蓄積されているフレームの再生、一時停止、停止、逆再生のモードを選択することができる。

【００３３】ここで、ユーザは、まず調査を行いたい日時や時刻を、キーボードやポインティングデバイスを用いて、また、日付・時刻情報表示エリア５１に直接触れる(液晶タッチパネルの場合)等によって、手動により任意に設定し、表示速度選択ボタン５２によって任意の速度を選択する。更に、作動ボタン５３を使って、再生、一時停止、停止、逆再生の操作を自由に行うことで、フレームを正順や逆順に表示させることができる。即ち、任意の時間経過後、あるいは指定した時刻からのカウントアップやカウントダウンを、任意の速度で表示させることが可能であり、また、終了や一時停止を自由に行うことができる。

【００３４】以上、詳述したように、本実施の形態によれば、フレームを構成するパケットのヘッダ部分から把握されたコンピュータ等の通信機器の論理的位置を、視覚的にユーザに対して表示することができる。また、ネットワーク内を流れる一つ一つのフレームにタイムスタンプを付与してリアルタイムでリストアップすることにより、フレームの通過時刻を把握することも可能である。更にまた、ディスプレイなどの表示装置に出力したり、プリンタ等の印字装置に出力することによって、複数のフレームにおける相互の関連性を視覚的に見て判断することができ、ネットワークを流れるフレームの状況を容易に分析、把握することができる。

【００３５】また、タイムスタンプを付与したフレームをハードディスク等の外部記録装置１２に全て蓄積することにより、蓄積されたフレームを時系列順でリストアップすることができる。更に、蓄積されたフレームを任意の速度で再生、一時停止、逆再生することによって、リアルタイムでリストアップした際に見逃したもの等をも含んで視覚的に見て判断することができ、フレームの状況を容易に分析、把握することができる。

【００３６】また、これらのフレームの流れを、線の太さや種類、色等を用いて種別して表示することで、ユーザにとっては、ネットワークの状況を視覚によって直感的に理解することが可能となる。また、例えば、不正かどうかが疑わしいフレームに対して色分けして表示することで、不正アクセスの発見も容易となる。

【００３７】尚、本実施の形態においてなされる各種処理は、ＣＤ-ＲＯＭ等の記憶媒体にプログラムとして格納することが可能であり、このＣＤ-ＲＯＭ等からフレーム監視装置として機能するコンピュータ装置にこのプログラムをインストールすることができる。かかる際には、コンピュータ装置に接続されたハードディスク等を外部記憶装置１２として利用し、また、接続されるディ

スプレイ等の表示装置をフレーム図化装置１４として利用することが可能である。

【００３８】

【発明の効果】以上説明したように、本発明によれば、ネットワーク内を流れる蓄積された任意の時間のフレーム、または現在流れているフレームをリアルタイムで視覚的に把握することができ、ネットワーク障害や不正アクセス等に対する分析および解析が容易となる。

【図面の簡単な説明】

【図１】　本実施の形態におけるシステムの全体構成を説明するための図である。

【図２】　本実施の形態における全体処理を説明するためのフローチャートである。

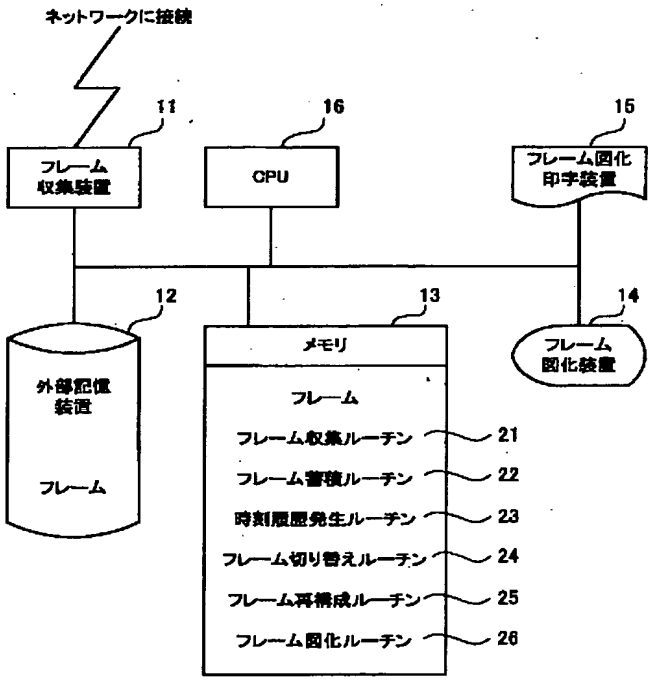
＊【図３】　フレーム図化装置１４等にて表示される表示例を示した図である。

【図４】　フレーム図化装置１４等で表示される設定画面の例を示した図である。

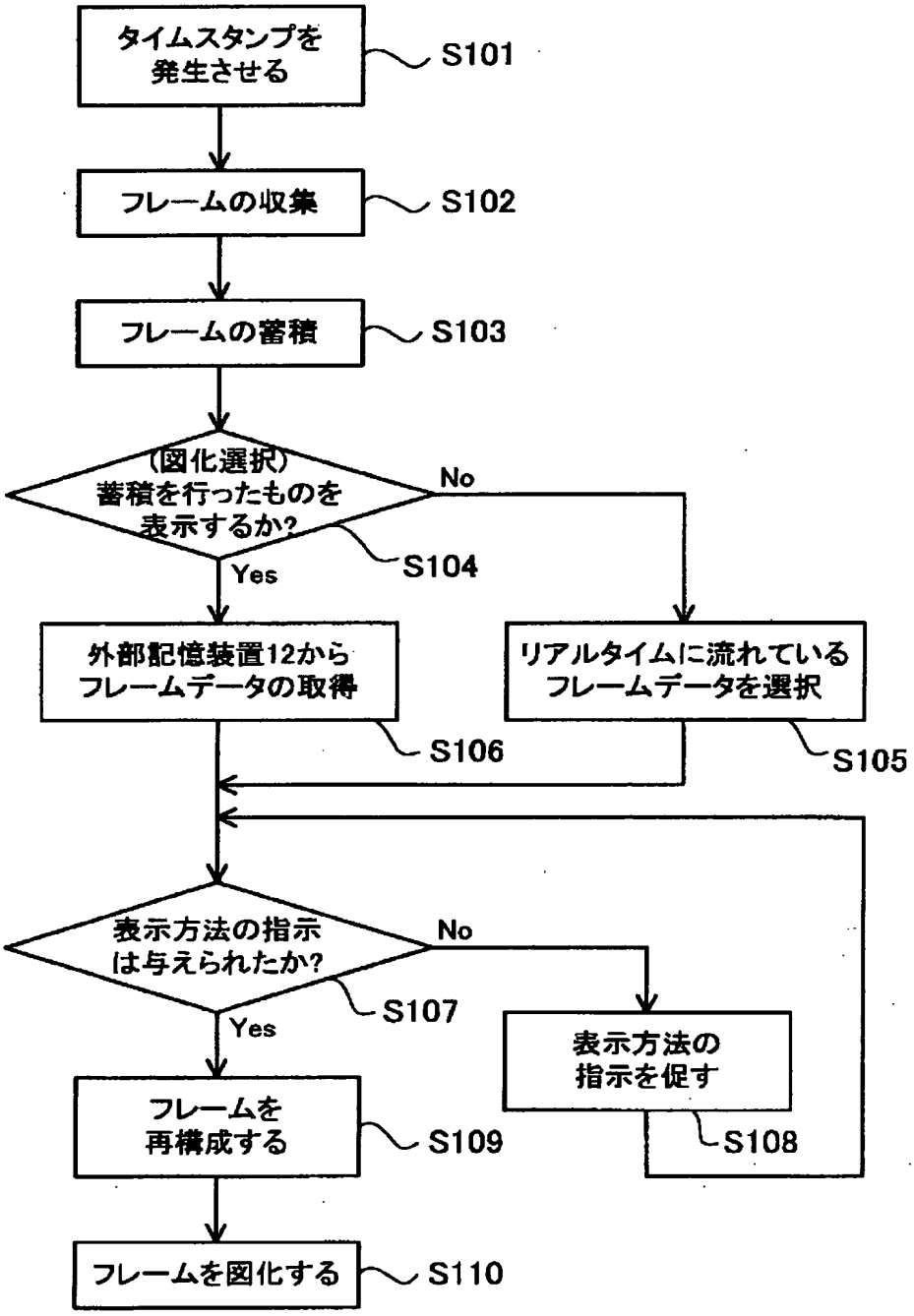
【符号の説明】

１１…フレーム収集装置、１２…外部記憶装置、１３…メモリ、１４…フレーム図化装置、１５…フレーム図化印字装置、１６…ＣＰＵ、２１…フレーム収集ルーチン、２２…フレーム蓄積ルーチン、２３…時刻履歴発生ルーチン、２４…フレーム切り替えルーチン、２５…フレーム再構成ルーチン、２６…フレーム図化ルーチン、３０、４０…画面、５０…設定画面

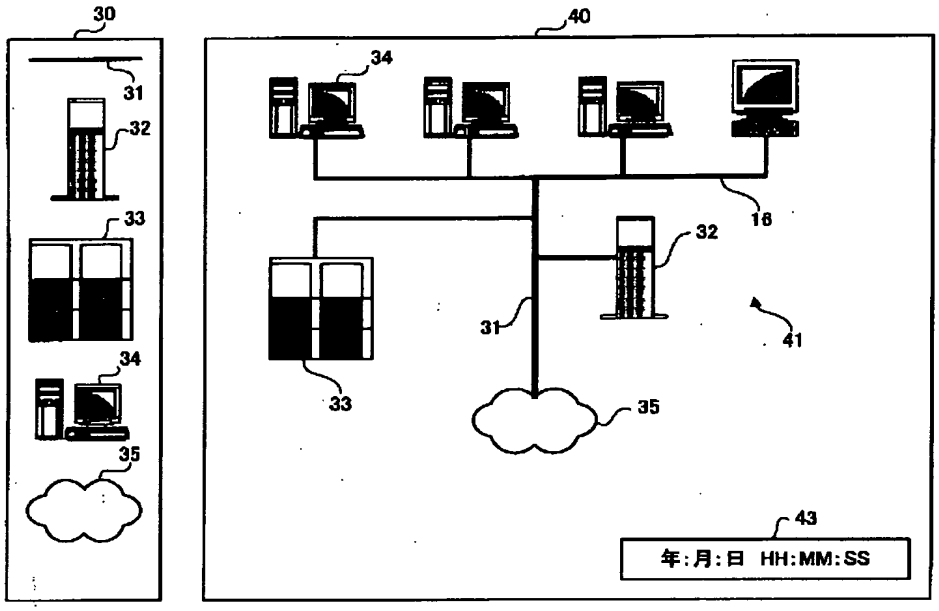
【図１】



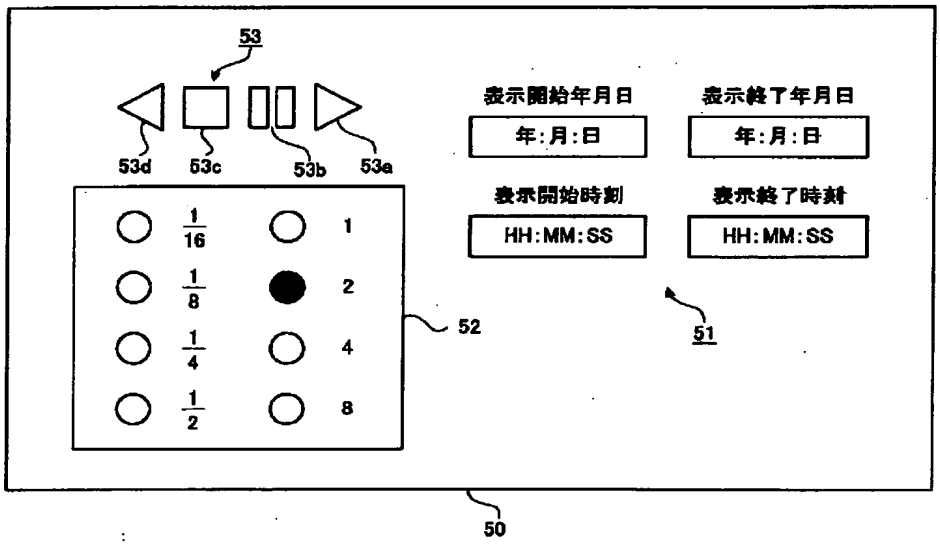
【図２】


タイムスタンプを発生させる
S101
フレームの収集
S102
フレームの蓄積
S103
(図化選択) 蓄積を行ったものを表示するか?
No
S104
Yes
外部記憶装置12からフレームデータの取得
リアルタイムに流れているフレームデータを選択
S106
S105
表示方法の指示は与えられたか?
No
S107
Yes
表示方法の指示を促す
フレームを再構成する
S109
S108
フレームを図化する
S110

【図３】


30
31
32
33
34
35
40
34
16
32
31
41
33
35
43
年:月:日 HH:MM:SS

【図４】


53
53d
53c
53b
53a
表示開始年月日
年:月:日
表示終了年月日
年:月:日
表示開始時刻
HH:MM:SS
表示終了時刻
HH:MM:SS
1/16
1/8
1/4
1/2
1
2
4
8
52
51
50

フロントページの続き

Ｆターム(参考) 5C054 AA10 DA06 EA03 FE00 GA01
HA00
5K030 GA14 GA18 HA08 HB15 HB16
HB18 JA10 KA07 LE11 MA04
MB01 MC08
5K033 AA05 CC01 DA01 DB12 DB20
EA06 EA07
5K035 AA03 AA07 BB03 BB04 DD01
EE02 EE21 GG13 JJ05 KK04
KK07 MM03